UHY Tokyo & Co
Certified Public Accountants

経産省：「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」の公表

UHY Tokyo ニュースレター / 2019年5月

経済産業省は2019年4月18日、「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を公表しました。本フレームワークは、政府が推進するサイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」の社会と、「Society5.0」の基盤となる「Connected Industries」の実現に向けて進展する次世代型のサプライチェーンである「価値創造過程（以下、バリュークリエーション）」において、セキュリティ対策の全体像を整理し、対策例をまとめたものです。概要は下記の通りであり、本フレームワークは下記URLからご確認いただけます。

https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

「Society5.0」の社会では、フィジカル空間とサイバー空間の融合によりフィジカル空間までサイバー攻撃が到達することが懸念されており、複雑につながるサプライチェーンにおいては影響範囲が拡大することが想定されています。本フレームワークの適用範囲は、従来型のサプライチェーンだけではなく、次世代型のサプライチェーンも含めた新たな産業社会であり、それぞれの組織の状況に応じてセキュリティ対策を選定することが可能となります。

本フレームワークは、以下3部と添付により構成されています。

第Ⅰ部 コンセプト

サイバーセキュリティの観点から、バリュークリエーションプロセスにおけるリスク源を整理するためのモデル（三層構造と６つの構成要素）を整理。

第Ⅱ部 ポリシー

第Ⅰ部で示したモデルを活用したリスク源の整理と、リスク源に対応する対策要件を提示。

第Ⅲ部 メソッド

第Ⅱ部で示した対策要件に対応するセキュリティ対策例を提示。

添　付

三層構造モデルを代表的な産業に適用した場合のユースケース、リスク源と対策要件の対応関係、対策要件に応じたセキュリティ対策例、海外の主要規格との対応関係、用語集

本フレームワークは、目指すべきセキュリティ対策の概念の整理に加え、各事業者がセキュリティ対策を実施する上で確認すべき方針を示している点で有用と思われます。一方で、セキュリティ対策は各産業分野でフォーカスする点が異なること、また中小企業においては対策にかけられる人的リソースの制約等もあり、社会全体でいかにして対策を実現していくかが今後の課題と考えられます。

ご質問やご要望がございましたらお気軽にお問い合わせください。

※なお、本稿の意見に関する部分は、筆者の個人的な見解であることをあらかじめお断りします。

コンタクト

UHY東京監査法人
小野　琢司 – IT・内部統制 PG
Email: takuji.ono@uhy-tokyo.or.jp

〒107-0052　東京都港区赤坂 7-3-37 プラース・カナダ 3F
Tel: +81 3 5410 1391 / Fax: +81 3 5410 2474
Website : http://www.uhy-tokyo.or.jp/